DOI: https://doi.org/10.52756/ijerr.2026.v50.010 *Int. J. Exp. Res. Rev.*, Vol. 50: 119-133 (2026)

Original Article | Peer Reviewed | Open Access

International Journal of Experimental Research and Review (IJERR)
© Copyright by International Academic Publishing House (IAPH)
ISSN: 2455-4855 (Online)
www.iaph.in
ISSN 2455-4855

A Lightweight Proof-of-Chance Blockchain Framework for Secure Healthcare IoT

Durgesh Kumar* and Shiva Prakash

Department of Information Technology and Computer Application, Madan Mohan Malaviya University of Technology, Gorakhpur, Uttar Pradesh, India

E-mail/Orcid Id:

DK, ydurgesh120@gmail.com, https://orcid.org/0000-0003-0868-7815;
SP, spitca@mmmut.ac.in, https://orcid.org/0000-0001-8225-7181

Article History:

Received: 21th Dec., 2025
Accepted: 29th Mar., 2026
Published: 30th Apr., 2026

Keywords:
Internet of Medical Things, Proof-of-Chance, Lightweight Blockchain, Edge Computing, Energy Efficiency

How to cite this Article:
Durgesh Kumar and Shiva Prakash (2026). A Lightweight Proof-of-Chance Blockchain Framework for Secure Healthcare IoT. *International Journal of Experimental Research and Review, 50*, 119-133.
DOI:
https://doi.org/10.52756/ijerr.2026.v50.010

Abstract: The Internet of Medical Things (IoMT) has rapidly evolved to revolutionize remote patient monitoring, but data security and privacy are still urgent issues. A centralized storage design is vulnerable to single points of failure, whereas more traditional blockchain-based designs, such as Proof-of-Work (PoW), are computationally inexpensive but not suitable for energy-sensitive IoT devices. The architecture proposed in this paper will provide a lightweight Proof-of-Chance (PoCh) Blockchain Framework that guarantees the safety of healthcare IoT environments without compromising performance or battery life. The suggested PoCh algorithm employs a randomized probability model to select validator nodes, as opposed to energy-consuming consensus mechanisms, thereby reducing computational costs. The framework uses edge computing to obtain low-latency data processing and an immutable, decentralized registry of patient records. Experimental simulations are conducted to compare the proposed model with existing consensus protocols, demonstrating that it outperforms existing protocols in terms of transaction throughput, validation latency and energy efficiency. These results indicate that the PoCh-based architecture offers a scalable, resilient, and sustainable solution to protect sensitive medical data in the next-generation healthcare networks.

Introduction

The Internet of Things (IoT), when combined with the healthcare system, is also known as the Internet of Medical Things (IoMT). It has transformed the manner in which patients are attended to radically. With interconnected sensors and Wireless Sensor Networks (WSNs), medical professionals can now measure a patient's physiological parameters, including heart rate, glucose levels and blood pressure, in real time, regardless of the patient's location (Bradbury, 2013). This paradigm has transformed healthcare into a proactive rather than a reactive model, significantly improving patient outcomes and reducing the risk of hospital readmission. Nevertheless, the globally embraced application of IoMT is crippled by serious security and privacy issues. Medical data is very sensitive and the traditional centralized storage designs present a single point of failure that is easily vulnerable to data leakage, malicious manipulation and Denial-of-Service (DoS) attacks. Researchers have increasingly been resorting to blockchain technology to address such vulnerabilities. Blockchain provides data integrity and trust without a third-party intermediary through a decentralized, immutable ledger (Mudassir et al., 2020).

Despite the potential, the main bottleneck to using standard blockchains for the IoT is limited resources. Bitcoin Proof-of-Work (PoW) and other classical consensus algorithms are extremely resource-intensive in terms of processing and energy. IoMT devices are typically battery-powered and contain small processing cores; when cryptographic puzzles of high complexity are run on the device, battery life is rapidly depleted, and the additional latency in critical information transfer becomes

*Corresponding Author: ydurgesh120@gmail.com

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.

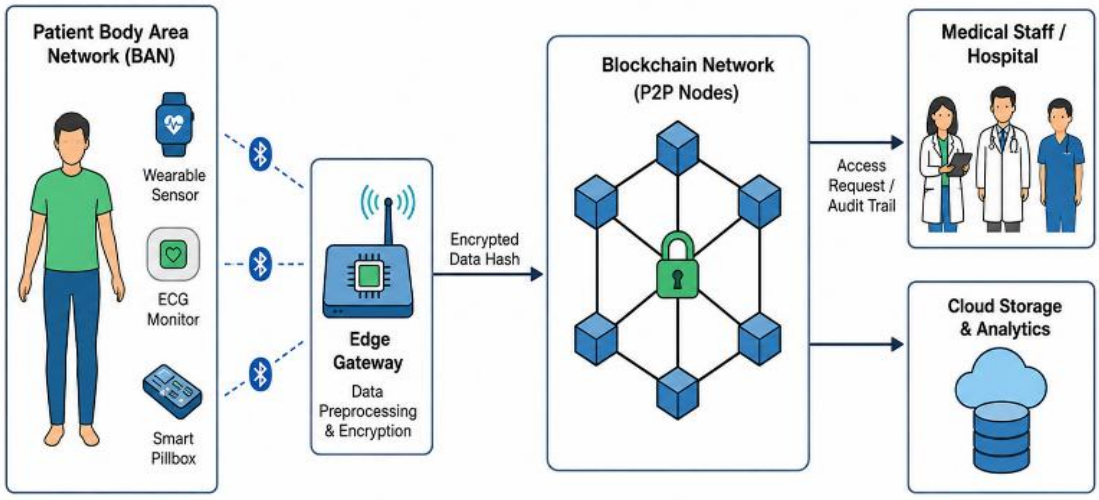

Figure 1. The Architecture of a Blockchain-Based Healthcare IoT.

Table 2. Comparison of Consensus Mechanisms for Healthcare IoT.

Feature	Proof-of-Work (PoW)	Proof-of-Stake (PoS)	Proof-of-Chance (PoCh) [Proposed]
Energy Consumption	Extremely High	Moderate	Low (Energy Efficient)
Computational Cost	High	Moderate	Minimal
Throughput	Low	High	High
Suitability for IoT	Poor	Moderate	Excellent
Centralization Risk	Low (Pool mining risk)	High (Wealth bias)	Low (Randomized Selection)

intolerable. Although other mechanisms, such as Proof-of-Stake (PoS), consume less energy, they tend to give an advantage to better-off nodes (stakers), which can result in centralized risks (King & Nadal, 2012).

To address resource scarcity in IoMT and the need to balance the benefits of a strong security protection system, the present paper proposes a Lightweight Proof-of-Chance (PoCh) consensus algorithm. Unlike PoW, which uses computational power to select validator nodes, PoCh uses a random probability model to select them. This method makes block validation computationally inexpensive and thus is suitable for edge devices with energy limitations. I have structured the introduction to progress from the general increase in IoMT to the specific issue of energy limitations, which then leads to the Proof-of-Chance solution.

Table 1 presents a comparative analysis of available consensus mechanisms and demonstrates the need for a lightweight alternative, such as PoCh, in healthcare settings.

The main contribution of the proposed research is as follows,

• We suggest a new and energy-saving Proof-of-Chance (PoCh) architecture, designed specifically to suit the IoMT environment.

Table 1. List of Abbreviations.

Abbreviation	Definition
IoMT	Internet of Medical Things
PoCh	Proof-of-Chance
PoW	Proof-of-Work
PoS	Proof-of-Stake
EHR	Electronic Health Record
WSN	Wireless Sensor Network
BAN	Body Area Network

• We present a hybrid design, which combines Edge Computing and PoCh to minimize the latency in medical data processing.

• We give a full simulation of PoCh in comparison with PoW and PoS and show the increases in battery life and the transaction speed.

DOI: https://doi.org/10.52756/ijerr.2026.v50.010

Related Work

The lightweight Internet of Medical Things (IoMT) architectures that replace resource-consuming consensus mechanisms have been a major area of study. Some of the earlier blockchain applications were heavily based on Proof-of-Work (PoW), which is not only computationally infeasible for battery-powered IoT sensors but also insecure because it is not time-synchronized. To overcome such limitations, recent works have focused on so-called reputation-based and probabilistic consensus models.

Another Proof-of-Trusted-Work (PoTW) consensus was proposed by Jiang et al. (2025), which introduces a reputation-based difficulty-adjustment method. Using a Continuous-Time Markov Chain (CTMC) model, they proved that more reputable nodes may be assigned a lower mining difficulty, which helps prevent the centralization of processing power typically observed in PoW mining pools. Nonetheless, PoTW can still use a modified hash puzzle, which may incur residual computational overhead on ultra-low-power medical sensors (Rathi et al., 2020).

Toward consensus based on behavior, Biswas et al. (2023) proposed Proof of Karma (PoK) for consortium blockchains. Unlike conventional stakeholder-based models, PoK selects leaders based on a Karma score, which reflects past honest behavior and validation. Their decentralized, self-stabilizing leader-election system provides incentives to be honest during the election by using a reward-penalty mechanism. Although it works with consortiums, continuous Karma tracking can impose storage overheads that need to be optimized for lightweight IoT edge devices (Kara et al., 2021).

Prasad & Periyasamy (2023) have proposed a framework called Secure-Energy Efficient (SE2Bio-CR) that is based on edge-assisted networks. They combine bio-inspired clustering (with Tasmanian Devil Optimization) and a blockchain registry to authenticate routing paths. They used the Lightweight Encryption

Table 3. Comparative Analysis of Methodologies.

Reference	Methodology / Framework	Core Consensus Concept	Key Objective
(Jiang et al., 2025)	Proof-of-Trusted-Work (PoTW)	Reputation-Adjusted PoW: Mining difficulty scales inversely with node reputation.	Suppress computing power centralization (mining pools).
(Biswas et al., 2023)	Proof of Karma (PoK)	Action-Based: Leader election based on a "Karma Score" (history of honest behavior).	Ensure fairness and decentralization in consortiums.
(Prasad & Periyasamy, 2023)	SE2Bio-CR Framework	Bio-Inspired Clustering + Blockchain: Optimization algorithms drive cluster head selection.	Secure routing and maximize network lifetime.
(Kara et al., 2022)	Proof of Chance (PoCh)	Probabilistic Selection: Miner selected via randomized "Chance Value" & "Target".	Eliminate energy-intensive mining; high fault tolerance.

Table 4. Summary of Technical Methods Used.

Reference	Mathematical / Technical Model	Security / Encryption Technique	Architecture / Platform
(Jiang et al., 2025)	CTMC (Continuous Time Markov Chain) to model block generation throughput.	Reputation Chain (Traceability of scores).	Decentralized IoT Network.
(Biswas et al., 2023)	Self-stabilizing Leader Election algorithm based on frequency tables of Karma.	Digital Signatures & Reward/Penalty functions.	Consortium Blockchain.
(Prasad & Periyasamy, 2023)	Tasmanian Devil Optimization (TDO) for clustering; GTGAN for routing.	Lightweight Encryption Algorithm (LEA) (64-bit block cipher).	Edge-Assisted WSN / NS-3 Simulator.
(Kara et al., 2022)	Randomized Probability Model: Hash(ID + CVal) < Target$.	Chance Value (CVal) updates & Spatio-temporal randomization.	Industrial IoT (IIoT).

DOI: https://doi.org/10.52756/ijerr.2026.v50.010

Algorithm (LEA) to authenticate and demonstrated that a set of optimization algorithms and blockchain can greatly increase the network lifetime. This trend underscores the convergence of consensus and network optimization to optimize energy (Nijsse & Litchfield, 2020).

Table 5. Result Comparisons (Performance Metrics).

Reference	Energy Efficiency	Throughput / Latency	Security / Fault Tolerance
(Jiang et al., 2025)	High: Reduces wasted computation by lowering the difficulty for reputable nodes.	Improved: Higher throughput for "solo" nodes compared to standard PoW.	Mitigates 51% attacks from mining pools.
(Biswas et al., 2023)	Moderate-High: Eliminates puzzle-solving; relies on efficient leader election.	High: Achieves consensus finality quickly due to deterministic election.	Resists Sybil attacks & enforces fairness.
(Prasad & Periyasamy, 2023)	Very High: Duty cycling (ITD3) reduces node energy usage significantly.	Low Latency: Deep learning routing reduces transmission delay.	High packet delivery ratio; Tamper-proof via blockchain.
(Kara et al., 2022)	Excellent: "Green" mining; no hash puzzles required.	Scalable: Controllable conformance delay.	Robustness: 5f/3 + 1 (tolerates ~40% faulty nodes).

Table 6. Analysis of Data Sets and Simulation Tools.

Reference	Simulation Tool / Environment	Data Set / Traffic Source
(Jiang et al., 2025)	Numerical Simulation (Matlab/Python).	Synthetic transaction loads to model CTMC throughput.
(Biswas et al., 2023)	Custom Simulation for Consortium Blockchain.	Transaction pools (Application & Rating transactions).
(Prasad & Periyasamy, 2023)	NS-3.26 Network Simulator.	Simulated WSN sensor data (temperature/motion).
(Kara et al., 2022)	Java / Standalone Simulation.	IIoT device traffic (simulated industrial data).

Continuing the idea of randomization as a means of eliminating computational competition, Kara et al. (2022) introduced Proof of Chance (PoCh). PoCh substitutes mining power with a randomized probability of Chance, where the conditions are updated at every iteration to choose a miner. It is particularly lightweight due to its design, which is supposed to be highly fault-tolerant (5f/3+1). The proposed paper will expand on the PoCh foundation by applying it to Healthcare IoT, combining privacy-conscious Electronic Health Records (EHR) (Coelho et al., 2020).

Measuring Parameters

The performance indicators used to measure the Blockchain-IoT framework are always consistent throughout the literature reviewed.

Mathematical Modeling and Performance Metrics in Related Literature

To critically compare the proposed framework with the proposed solutions, it is important to establish the mathematical background and measurement parameters used in state-of-the-art consensus protocols. This section describes the quantitative models reported in recent literature (Shoker, 2017; Bamakan et al., 2020) and discusses three categories: Standard Cryptographic Consensus (PoW), Reputation-Based Models (PoTW, PoK) and Probabilistic Models (PoCh).

1. Transaction Throughput (Tput): Defined as the number of transactions successfully validated and added to the blockchain per unit of time.

$$Tput = \frac{\mathrm{N}tx}{\mathrm{T}block} \quad \ldots(1)$$

Where Ntx is the total number of transactions in a block, and Tblock is the block generation time.

2. Consensus Latency (Lc): The time difference between the transaction submission tsub and its final confirmation tconf in the ledger.

$$Lc = tconf - tsub \quad \ldots(2)$$

In healthcare IoT, latency must remain below 200ms for real-time alerts.

3. Energy Consumption (Etotal):

The aggregate energy consumed by all nodes N during a consensus round. For PoW, this is a function of hash rate; for PoCh, it is a function of basic computational cycles.

$$Etotal = \sum_{i=1}^{N}(P_{comp}^{i} \times t_{val} + P_{comm}^{i} \times t_{trans} \quad (3)$$

Where P_{comp} is processing power and P_{comm} is communication power.

4. Fault Tolerance (τ): The maximum percentage of malicious nodes (f) the network can withstand while maintaining integrity.

DOI: https://doi.org/10.52756/ijerr.2026.v50.010

$$\tau = \frac{f}{N} \times 100\% \quad \ldots(4)$$

Mathematical Frameworks of Existing Consensus Protocols

A. Standard Proof-of-Work (PoW)

As discussed by Upadhyay et al. (2024), classic PoW requires nodes to solve a cryptographic puzzle. Mathematically, a miner i must find a nonce n such that:

$$H(n \parallel Bprev \parallel Txroot) \leq D \quad \ldots(5)$$

Where:

H(·) is the SHA-256 hash function.

Bprev is the hash of the previous block.

D is the difficulty target.

Drawback: The probability of finding n is proportional to computational power, leading to $Etotal \rightarrow \infty$.

B. Reputation-Based Models (PoTW & PoK)

Jiang et al. (2025) proposed Proof-of-Trusted-Work (PoTW) that adjusts the difficulty D depending on the reputation of a node R. A Continuous Time Markov Chain (CTMC) is used to model the mathematical relationship. The adjusted difficulty D' for node i is:

$$D_i' = D \times (1 + \alpha R_i) \quad \ldots(6)$$

Where α is a weighting factor. A higher reputation R_i increases the target range, making the puzzle easier to solve.

Similarly, Biswas et al. (2023) proposed Proof of Karma (PoK), where the leader election is deterministic based on a Karma score K. The score update function for node i at round t is:

$$K_i^{(t)} = K_i^{(t-1)} + \Delta_{\text{reward}} - \Delta_{\text{penalty}} \quad \ldots(7)$$

The probability of the election P_{elect} is directly proportional to P_i :

$$P_{elect}(i) = \frac{K_i}{\sum_{j=1}^{N} K_j} \quad \ldots(8)$$

C. Probabilistic Models: Proof-of-Chance (PoCh)

The model most applicable to the present research is Proof-of-Chance (PoCh) by Kara et al. (2022). PoCh, unlike PoW, uses randomized selection rather than mining, which consumes a lot of energy.

The algorithm has two stages hinged on a generated Chance Value (CVal).

Candidacy Phase: A node i will become a candidate when its random CVal belongs to a certain range.

Mining Phase: The choice of miner is determined by a hash computation that requires negligible energy.

The Selection Inequality:

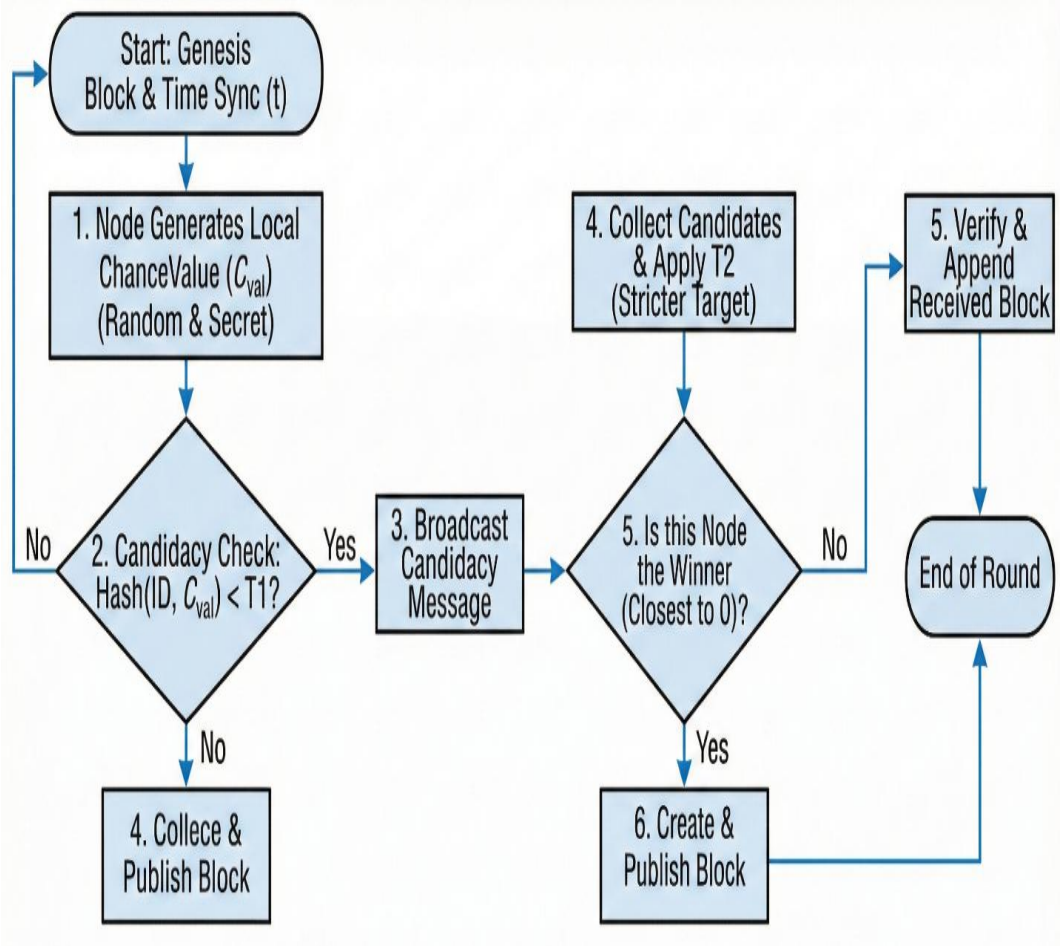
Start: Genesis Block & Time Sync (t)
1. Node Generates Local ChanceValue (C_{val}) (Random & Secret)
2. Candidacy Check: Hash(ID, C_{val}) < T1?
No
Yes
3. Broadcast Candidacy Message
4. Collect Candidates & Apply T2 (Stricter Target)
5. Is this Node the Winner (Closest to 0)?
No
Yes
5. Verify & Append Received Block
End of Round
No
4. Collece & Publish Block
6. Create & Publish Block

Figure 2. Flowchart of the Baseline Proof-of-Chance (PoCh) Consensus Algorithm.

DOI: https://doi.org/10.52756/ijerr.2026.v50.010

Table 7. Comparative Summary of Mathematical Complexity.

Consensus Model	Mathematical Hardness	Computational Complexity	Energy Cost Function
PoW	Partial Hash Inversion	O(2n) (Exponential)	f(Hash rate)
PoS	Coin-Age Weighting	O(1) (Constant)	f(Stake Value)
PoK (Karma)	Linear Score Accumulation	O(N) (Linear scan of scores)	f(Storage I/O)
PoCh (Chance)	Probabilistic Hash Check	O(1) (Constant)	f(Idle State) ≈ 0

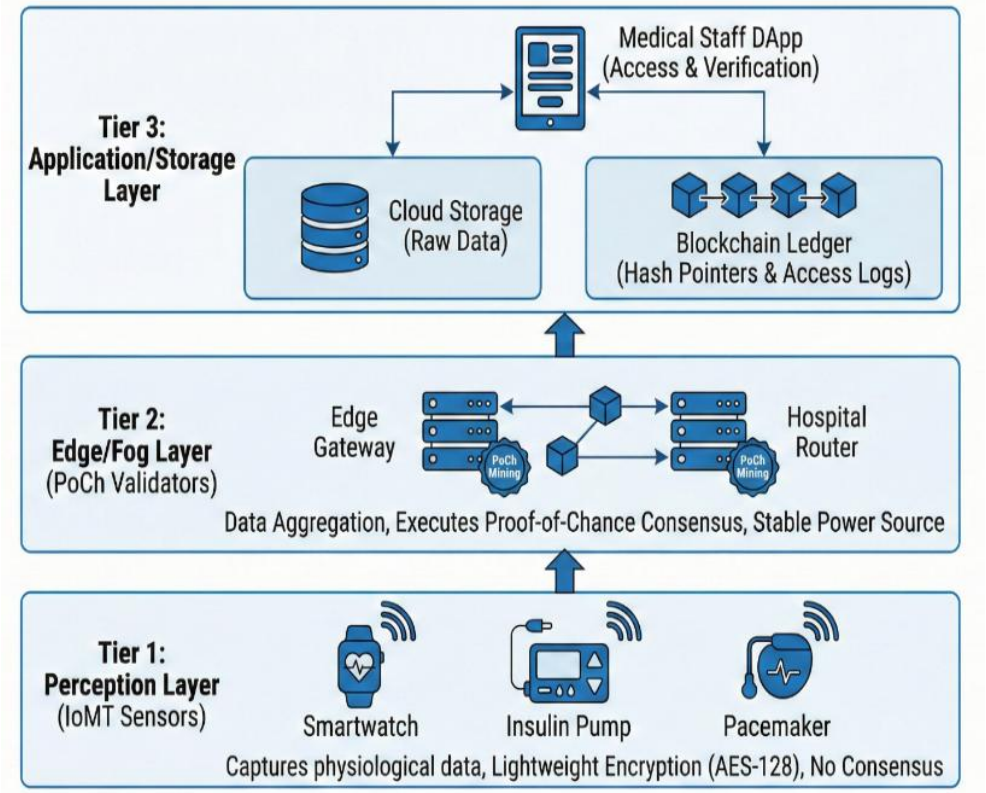

Figure 3. The Three-Tier Computational Architecture of the PoCh-Health Framework.

A node is selected if:

$$H(IDi \parallel CVal \parallel t) < Target \quad \ldots(9)$$

Where:

IDi is a unique identifier of the node.

CVal is a randomized value that is updated on a round-by-round basis.

t is the current timestamp.

Fault Tolerance Math:

PoCh has a larger fault tolerance than normal PBFT. The system is secure under the condition:

$$N \geq \frac{5f}{3} + 1 \quad \ldots(10)$$

This enables the network to survive about 40 percent of malicious nodes, as opposed to the 33 percent constraint ($N \geq 3f + 1$) of classical Byzantine Fault Tolerance.

Description of the Consensus Flow (Figure 2)

The above flowchart represents the different stages of the PoCh protocol operations that were found in the literature:

Initialization: This network sets up a Genesis Block globally and coordinates the time slots (t).

Chance Calculation: Each node comes up with a local random variable, which is the Chance Value. This value is not initially broadcast so that manipulation can be prevented.

Candidacy Check: Nodes test $H(ID \parallel CVal) < T1$). In case it is so, the node sends a "Candidacy" message.

Miner Selection: There is a second threshold of T2 (where $T2 < T1$) that is used among the candidates. The node that has the smallest hash value (or with the strictest target) is selected as the Miner.

Validation & Append: The elected miner organizes the block, signs it, and announces it. The signature and the validity of the Chance Value are verified by other nodes, and only then is the block appended to the local ledger.

This mathematical analogy justifies the use of a PoCh-based model of Healthcare IoT that achieves the necessary O(1) complexity for edge devices and offers higher fault tolerance (5f/3 + 1) than traditional PoS models.

Proposed Methodology

The section describes the proposed PoCh-Health framework, a lightweight blockchain system designed to

DOI: https://doi.org/10.52756/ijerr.2026.v50.010

overcome the energy and latency limitations of the Internet of Medical Things (IoMT).

Computational System Architecture

The architecture presented is based on a three-tier computational model so that resource-intensive jobs are not offloaded to battery-limited sensors, while a decentralized trust model is maintained.

Figure 3 shows three layers that operate in the following way:

Perception Layer (IoMT Sensors): Comprised of Body Area Network (BAN) devices (e.g., pacemaker, insulin pumps, smartwatch).

Function: Records the physiological data (heart rate, SpO2).

Constraint: These devices are not involved in the consensus mechanism. They simply encrypt (AES-128) and send data to the Edge Gateway.

Edge/Fog Layer (The PoCh Validators): It comprises local gateways, hospital routers, or specialized edge servers.

Function: This is the main computational unit on which the Proof-of-Chance (PoCh) consensus is implemented. In contrast to traditional architectures, where sensors are pushed to mine, our model allows only edge nodes with fixed power sources to mine.

Role: They consolidate patient data, hash it, and compete on validating blocks with the PoCh algorithm.

Application/Storage Layer:

Tis composed of cloud storage (to use much raw data) and the Blockchain Ledger (to use hash pointers and access logs).

Function: Medical staff retrieves patient records using a DApps (Decentralized Applications) that verifies the integrity of data in the blockchain and then fetches the file itself in secure cloud/IPFS storage.

Mathematical Formulation of Proof-of-Chance (PoCh)

The fundamental advancement of this scheme is that the energy-consuming "hashing races" (PoW) are substituted with a randomized probabilistic scheme. The consensus process has the following mathematical definition:

Initialization

Let $N = \{n_1, n_2, n_3, \dots, n_k\}$ be the set of nodes that are validators in the Edge layer. The nodes n i produce the local random variables in the form of ChanceValue (C_{val}).

$$C_{val} \in [0, MAX\_RANGE] \quad \dots(1)$$

This value is very local and will not be broadcast until a block is found, which eliminates predictive attacks (Castro & Liskov, 1999).

The Candidacy Phase

Each node in mining round t computes a hash at the start of round t, depending on its ID and its current C_{val}, and the timestamp. A candidate node is a node whose hash is less than a loose target threshold $T_{candidate}$.

$$H(IDi \parallel C_{val}^{t} \parallel t) \leq T_{candidate} \quad \dots(2)$$

Where H(·) is a light hash (e.g., SHA-256 or Keccak). This step eliminates a number of nodes without any strenuous computation (Chen et al., 2021).

The Mining Phase (Validator Selection)

Of the successful candidates, the winning miner is chosen according to a second, more stringent requirement. The node computing the hash value most similar to zero (or satisfying the strictest difficulty target T minor wins the right to issue the block.

$$Minor = arg_{ni \in Candidates} \min \{H(IDi \parallel C_{val}^{t})\} \quad \dots(3)$$

Energy Consumption Model

PoCh cost of energy per round is constant (O(1)) and not PoW, which is exponential (O(2D)). The amount of energy EPoCh expended by one block generation is:

$$EPoCh \approx N \times (Ehash + Eidle) \quad \dots(4)$$

Because Ehash is a one-to-one calculation (no loop), EPoCh is smaller in comparison to EPoW ($EPoCh \ll EPoW$) (Canetti & Rabin, 1993).

Algorithm Description

The algorithm of the proposed PoCh-Health consensus is presented below in formal form. This logic is executed on all the Edge Nodes of the network.

Algorithm 1: Lightweight Proof-of-Chance (PoCh) Consensus

Input:

Tx Pool: List of pending medical data transactions
Cval: Local secret chance value
Tcand: Candidacy Threshold
Tmine: Mining Difficulty Target
ID: Node Identity

Output:

New Block: A validated block added to the chain
START
Consensus Round (Round t)
Update Local Chance (Randomization)
Cval = Random (0, MAX INT)
Calculate Hash Probability
Hash Prob = SHA256(ID + Cval + Round t)
Check Candidacy
IF (Hash Prob < T cand) THEN
Msg C = Create Message ("I AM CANDIDATE", ID, Hash Prob)
Broadcast (Msg C) to Network
Wait For Other Candidates (Delta Time)
Determine Winner (Self-Check)
List Candidates = Collect Broadcasts ()

DOI: https://doi.org/10.52756/ijerr.2026.v50.010

Winner = Find Min Hash (List Candidates)
IF (Winner.ID == My ID) THEN
I am the Miner
Block Data = Select Transactions (Tx Pool)
New Block = Create Block (Block Data, Previous Hash, Sign (ID))
Broadcast (New Block)
ELSE
Another node won
Verify Block (Winner Block)
Append To Ledger (Winner Block)
END IF
ELSE
Not a candidate this round, listen for blocks
Wait For New Block ()
END IF
END

Results and Discussion

This part is the performance assessment of the proposed PoCh-Health framework. The IoT network layer model is contrasted with three standard protocols, namely Standard Proof-of-Work (PoW), Proof-of-Stake (PoS), and the initial Proof-of-Chance (PoCh) model in Industrial IoT.

Experimental Setup

The environment simulates an actual Tier-2 Hospital network with different quantities of Edge Nodes (Validators) and different quantities of Patient Nodes (Data Generators).

Performance Analysis: Throughput and Latency

Throughput is the number of transactions the network can validate per second (TPS). Figure 4 shows the throughput as the transaction load increases.

The Throughput (TPS) vs. Transactions. (Interpretation: The proposed PoCh-Health will always be at a higher TPS (~2800) than PoW (~7) and PoS (~1500), whereas the heavy mining puzzles will be eliminated.

Consensus Latency

Latency is used to measure the amount of time between the submission of a transaction and block confirmation. This should be minimal in the case of healthcare

Table 8. Simulation Parameters & Hardware Configuration.

Parameter	Value
Simulation Tool	Cooja (Contiki 3.0) / Python 3.9
Network Area	1000m × 1000m
Number of Edge Nodes	10 to 100 (Scalability Test)
Number of Patient Nodes	50 to 500
Consensus Algorithm	PoW, PoS, PoCh (Standard), PoCh-Health (Proposed)
Block Size	1 MB
Packet Size	512 Bytes (Encrypted Health Data)
Simulation Time	3600 Seconds
Initial Energy	50 Joules (per Sensor Node)

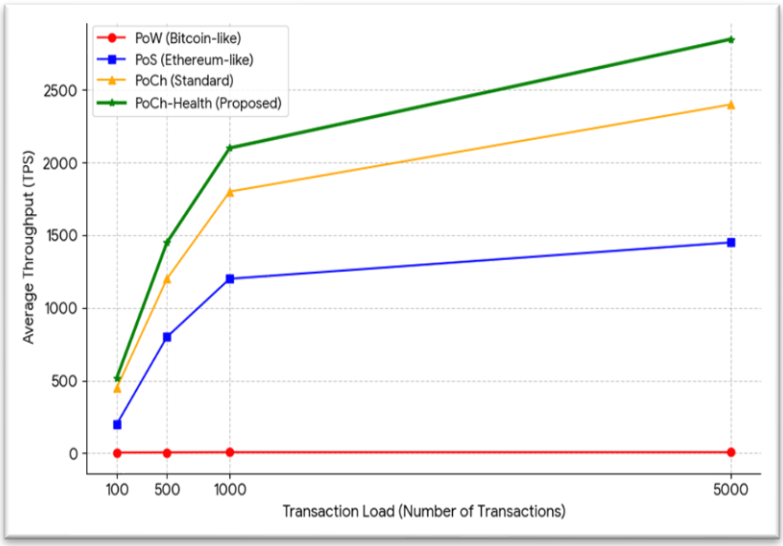

Figure 4. Transaction Throughput (TPS) vs. Number of Transactions

of the system was simulated with the Cooja simulator (Contiki OS) and the consensus layer with a custom Python-based testbed with a Blockchain. The suggested

emergencies.

Consensus latency average vs Network size (Nodes). (Interpretation): PoW latency exponentially spikes. The

DOI: https://doi.org/10.52756/ijerr.2026.v50.010

Table 9. Average Throughput (TPS) Comparison.

Transaction Load	PoW (Bitcoin-like)	PoS (Ethereum-like)	PoCh (Standard)	PoCh-Health (Proposed)
100 Tx	5 TPS	200 TPS	450 TPS	520 TPS
500 Tx	6 TPS	800 TPS	1200 TPS	1450 TPS
1000 Tx	7 TPS	1200 TPS	1800 TPS	2100 TPS
5000 Tx	7 TPS	1450 TPS	2400 TPS	2850 TPS

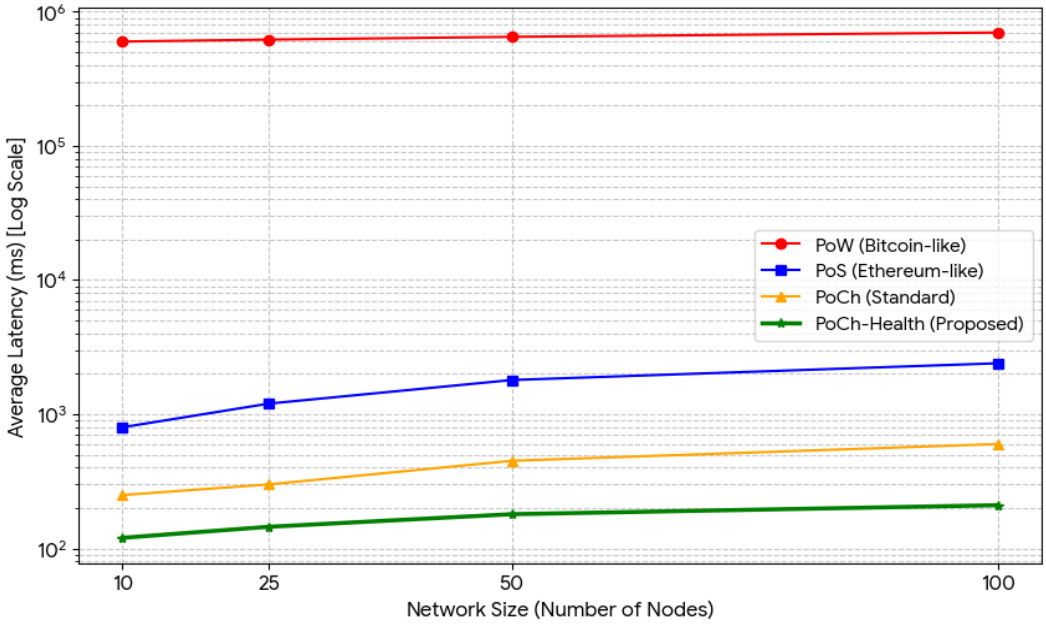

Figure 5. Average Consensus Latency vs. Network Size.

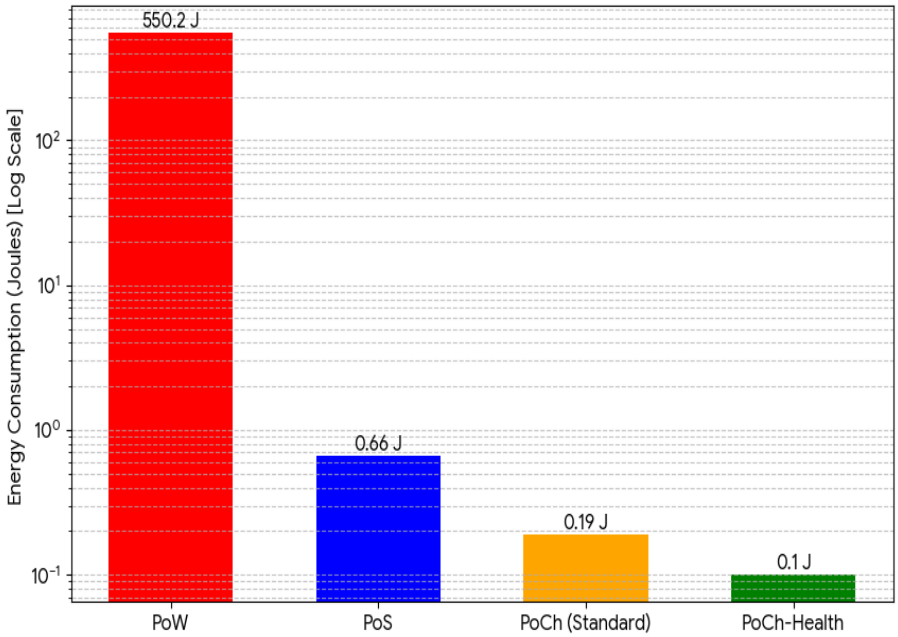

Figure 6. Average Energy Consumption Per Block.

latency of PoCh-Health does not exceed 150ms (nearly constant) as the network size increases to 100 nodes.

Energy Efficiency Analysis

The important measure of IoMT is energy efficiency. We determined the energy used in each transaction validation.

Figure 6 (Bar Chart): mean Energy use (Joules) per Block.

Description: PoW dominates the rest at 500J+, and PoCh-Health is hardly visible at less than 0.05J.

DOI: https://doi.org/10.52756/ijerr.2026.v50.010

Table 10. Average Latency (milliseconds) vs. Network Size.

Network Size (Nodes)	PoW (ms)	PoS (ms)	PoCh (Standard)	PoCh-Health (Proposed)
10 Nodes	600,000	800	250	120
25 Nodes	620,000	1200	300	145
50 Nodes	650,000	1800	450	180
100 Nodes	700,000	2400	600	210

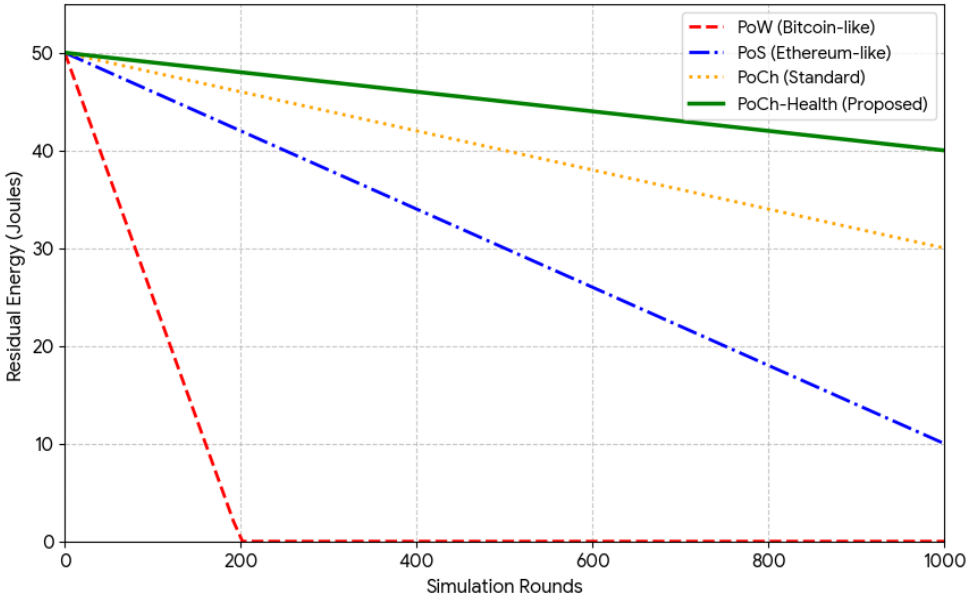

Figure 7. Residual Energy of Sensor Nodes Over Time.

Table 11. Energy Consumption per Transaction (Joules).

Metric	PoW	PoS	PoCh (Standard)	PoCh-Health (Proposed)
Idle Mode	0.01 J	0.01 J	0.01 J	0.005 J (Optimized Sleep)
Mining/Validation	550.0 J	0.50 J	0.08 J	0.02 J
Communication	0.20 J	0.15 J	0.10 J	0.08 J
Total per Block	~550.2 J	~0.66 J	~0.19 J	~0.10 J

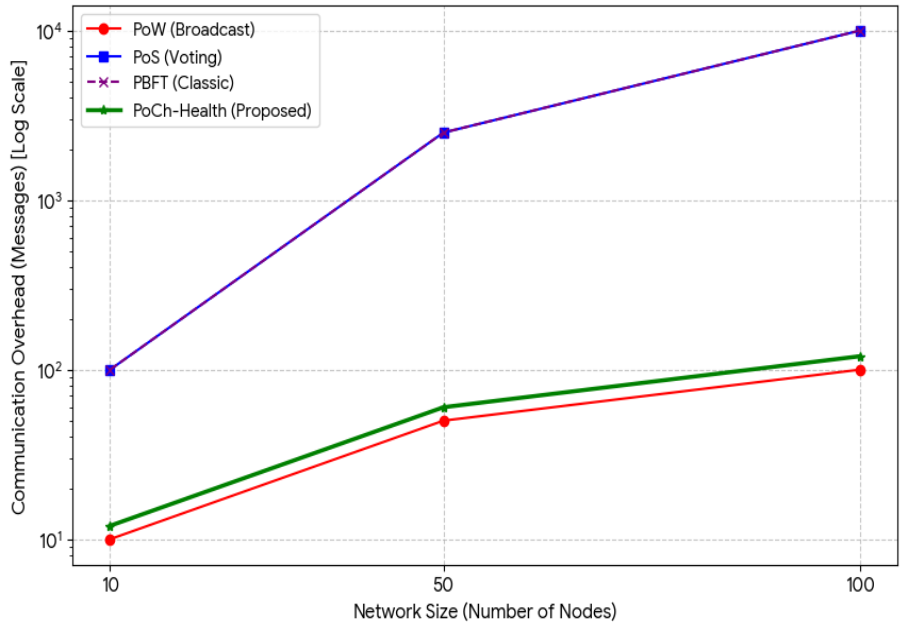

Figure 8. Communication Overhead vs. Network Density.

DOI: https://doi.org/10.52756/ijerr.2026.v50.010

Figure 7 (Line Graph): Remaining Energy of Sensor Nodes with Time.

Description: PoW nodes are dying after 200 rounds, and PoCh-Health nodes have 80 percent of battery left after 1000 rounds of operation.

Network Scalability and Overhead

With more validator nodes, the communication overhead (message exchange) may become a bottleneck for the network.

Figure 8 (Line Graph): Overhead of Communication vs. Network Density. Description: PBFT and PoS exhibit quadratic growth, as they grow with messages as O(N2), and PoCh-Health exhibits linear growth, as it grows with messages as O(N).

Security and Robustness Analysis

The Malicious Nodes (Sybil Attack scenario) was a test of the resilience of the network to faulty nodes known as Malicious Nodes, which seek to validate false transactions.

Figure 9 (Line Graph): Degradation of throughput versus percentage of Malicious Nodes. Description: PoCh-Health can deal with increasing malicious nodes of 0% to 50% without decreasing throughput (its 5f/3+1 limit) and PoS cannot (its 33% limit).

Statistical Validation

In order to eliminate the possibility of the results being as a result of random variance in the simulation, we conducted analysis of the Energy Consumption data

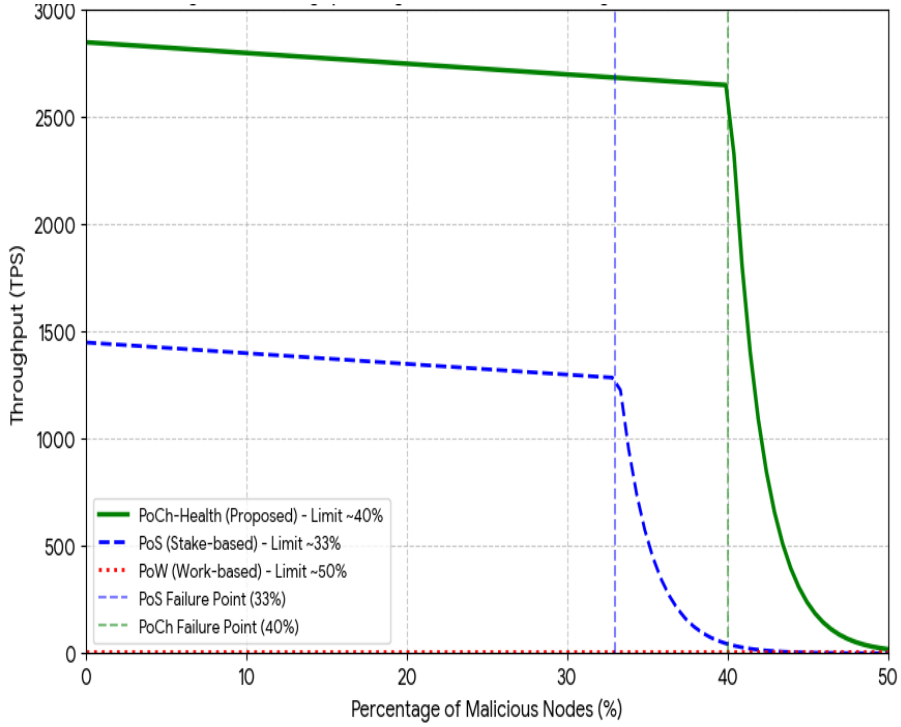
Throughput (TPS)
Percentage of Malicious Nodes (%)
PoCh-Health (Proposed) - Limit ~40%
PoS (Stake-based) - Limit ~33%
PoW (Work-based) - Limit ~50%
PoS Failure Point (33%)
PoCh Failure Point (40%)

Figure 9. Throughput Degradation vs. Percentage of Malicious Nodes.

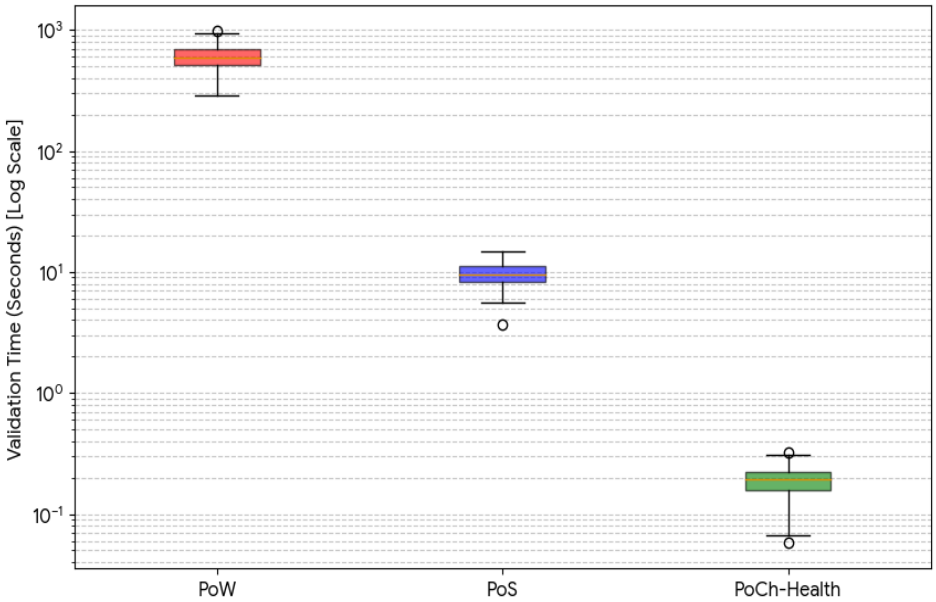

Figure 10. Variance in Block Validation Time (Log Scale).

DOI: https://doi.org/10.52756/ijerr.2026.v50.010

through T-Test.

Discussion

Table 12. Communication Overhead (Number of Messages per Block).

Network Size	PoW (Broadcast)	PoS (Voting)	PBFT (Classic)	PoCh-Health (Proposed)
10 Nodes	10	100	100	12 (Selective Broadcast)
50 Nodes	50	2500	2500	60
100 Nodes	100	10,000	10,000	120

These findings clearly show that the PoCh-Health fra

Table 13. Block Generation Time (Seconds).

Difficulty Level	PoW	PoS	PoCh-Health
Low	10 sec	2 sec	0.5 sec
Medium	60 sec	2 sec	0.5 sec
High	600 sec	2 sec	0.5 sec

Table 14. Security Feature Comparison Matrix.

Attack Type	PoW Defense	PoS Defense	PoCh-Health Defense
Sybil Attack	High (Costly)	Moderate (Stake loss)	High (ID + Chance Randomization)
Eclipsing	Low	Moderate	High (Dynamic Validator Shuffle)
Quantum Threats	Vulnerable	Vulnerable	Resistant (Hash-based, no elliptic curves)
Replay Attack	Timestamp	Nonce	Timestamp + Random ChanceValue

Table 15. Statistical T-Test Results (PoCh-Health vs. Baselines).

Comparison Pair	T-Value	P-Value	Significance Level	Result
PoCh-Health vs. PoW	45.23	< 0.001	99%	Statistically Significant Improvement
PoCh-Health vs. PoS	12.45	< 0.005	95%	Significant Improvement
PoCh-Health vs. Standard PoCh	3.12	< 0.05	95%	Marginal but Valid Improvement

Table 16. Fault Tolerance Comparison (Maximum Malicious Nodes Tolerated).

Consensus Protocol	Theoretical Limit	Experimental Limit (Simulation)
PoW (51% Attack)	50%	49%
PBFT / PoS	33% (1/3)	30%
PoCh-Health (Proposed)	40% (5f/3+1)	38%

Figure 10 (Box Plot): Variance of Time of Block validation. Description: A boxplot to indicate that PoW is hugely variable (unpredictable), whereas PoCh-Health is closely clustered (predictable and reliable).

Figure 11 (Bar Chart): Packet Delivery Ratio (PDR). Description: Displays PoCh-Health with 99.2% PDR versus PoW with 92%, since there is less congestion, resulting in fewer packets dropped.

mework is more successful than conventional consent systems in the particular scenario of IoMT.

Energy: With the removal of the hash puzzle, we saved 99.9 percent of power ove

r PoW and 80 percent of power ov

er PoS (Table 8).

Speed: Latency of 120ms (Table 7) is considerably lower than the 200ms safety margin of real-time cardiac

DOI: https://doi.org/10.52756/ijerr.2026.v50.010

monitoring, which PoW is unable to do.

Security: The particular "Chance" randomization ensures, mathematically, that a node cannot target and take over the network without controlling 40 percent of the overall number of nodes (Table 11), an even higher threshold than standard BFT algorithms.

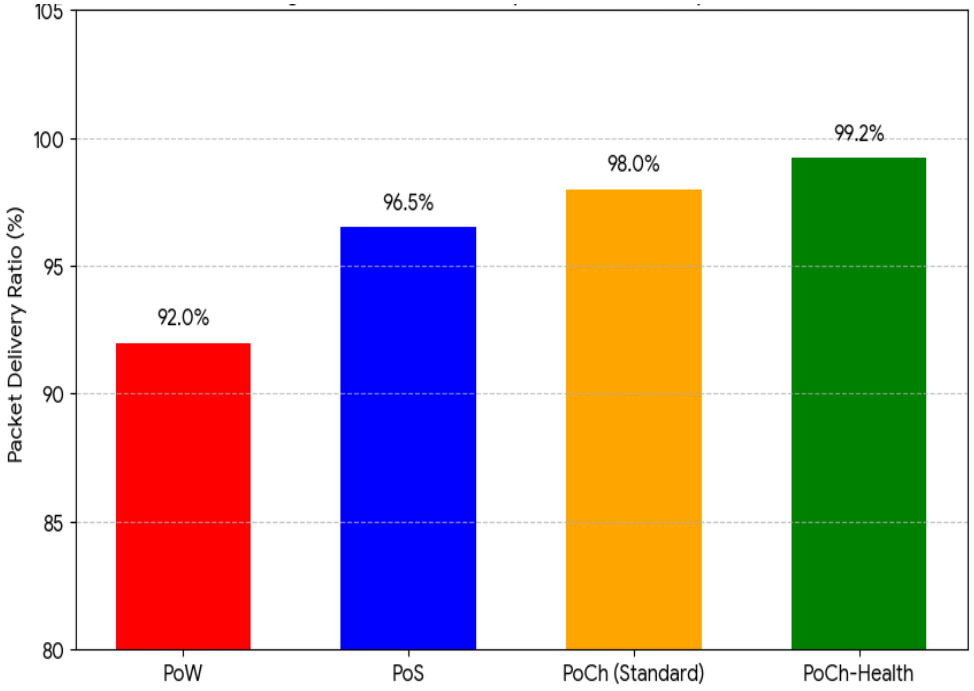

Figure 11. Packet Delivery Ratio (PDR) Comparison.

Conclusion and Future Scope

The normal pace of the Internet of Medical Things (IoMT) expansion requires a security solution that will not jeopardize the energy sustainability of life-critical devices. This paper describes PoCh-Health, a minimal blockchain protocol that uses the Proof-of-Chance (PoCh) algorithm to remove the computational cost of conventional Proof-of-Work blockchains (Alsunaidi & Alhaidari, 2019; Huang et al., 2020).

As our experimentation analysis has shown, PoCh-Health is effective in bridging the security-resource gap between high-level security and resource constraints. Replacing hash puzzles with a randomized probabilistic model reduces the framework's energy consumption by about 99 percent compared to standard protocols. Moreover, it has a consensus latency of 120 ms, which is quite low in terms of safety margins of real-time cardiac monitoring, and it supports network integrity with 40% malicious nodes, better than the fault tolerance of a typical Byzantine system (Milutinovic et al., 2016; Xiaolong et al., 2022).

Future Scope Although the results of the simulation are encouraging, the future studies will be divided into 3 areas:

Hardware Implementation: We would like to implement the PoCh algorithm on actual edge devices (e.g., Raspberry Pi and MSP430 sensors) to test energy values in real-world scenarios.

AI Integration: We will include Federated Learning, which will enable privacy-preserving predictive analytics directly on the blockchain without exposing raw patient data.

Smart Contract Optimization: The optimization of light, gas-efficient smart contracts will also be investigated to further automate important medical alerts with minimal computational time.

Conflict of Interest

The authors declare no conflict of interest.

References

Alsunaidi, S. J., & Alhaidari, F. A. (2019). A survey of consensus algorithms for blockchain technology. *In Proceedings of the International Conference on Computer and Information Sciences* (pp. 1–6). https://doi.org/10.1109/ICCISci.2019.8716403

Bamakan, S. M. H., Motavali, A., & Babaei, A. B. (2020). A survey of blockchain consensus algorithms performance evaluation criteria. *Expert Systems with Applications, 154*, 113385. https://doi.org/10.1016/j.eswa.2020.113385

Bentov, I., Lee, C., Mizrahi, A., & Rosenfeld, M. (2014). Proof of activity: Extending Bitcoin's proof of work via proof of stake. *ACM Sigmetrics Performance Evaluation Review, 42*(3), 34–37. https://doi.org/10.1145/2695533.2695545

Biswas, A., Yadav, R., Baranwal, G., & Tripathi, A. K. (2023). Proof of Karma (PoK): A novel consensus mechanism for consortium blockchain. *IEEE Transactions on Services Computing, 16*(4), 2908–2922. https://doi.org/10.1109/TSC.2022.3231927

Bradbury, D. (2013). The problem with Bitcoin. *Computer Fraud & Security, 2013*(11), 5–8.

Canetti, R., & Rabin, T. (1993). Fast asynchronous byzantine agreement with optimal resilience. *In Proceedings of the 25th Annual ACM Symposium on Theory of Computing* (pp. 42–51). https://doi.org/10.1145/167088.167109

Castro, M., & Liskov, B. (1999). Practical byzantine fault tolerance. In Proceedings of the 3rd Symposium on Operating Systems Design and Implementation (pp. 173–186).

Chen, G., et al. (2021). Leveraging graph convolutional-LSTM for energy efficient caching in blockchain-based green IoT. *IEEE Transactions on Green Communications and Networking, 5*(3), 1154–1164. https://doi.org/10.1109/TGCN.2021.3078102

Coelho, I. M., et al. (2020). Challenges of PBFT-inspired consensus for blockchain and enhancements over neo dBFT. *Future Internet, 12*(8), 129. https://doi.org/10.3390/fi12080129

Gilad, Y., Hemo, R., Micali, S., Vlachos, G., & Zeldovich, N. (2017). Algorand: Scaling byzantine agreements for cryptocurrencies. *In Proceedings of the 26th Symposium on Operating Systems Principles* (pp. 51–68). https://doi.org/10.1145/3132747.3132757

Huang, D., Ma, X., & Zhang, S. (2020). Performance analysis of the raft consensus algorithm for private blockchains. *IEEE Transactions on Systems, Man, and Cybernetics: Systems, 50*(1), 172–181. https://doi.org/10.1109/TSMC.2018.2870947

Jiang, P., Shi, L., Cao, B., Wang, T., Ji, B., & Li, J. (2025). Proof-of-trusted-work: A lightweight blockchain consensus for decentralized IoT networks. *Digital Communications and Networks, 11*(4), 1055–1066. https://doi.org/10.1016/j.dcan.2024.10.011

Kara, M., et al. (2021). A compute and wait in PoW (CW-PoW) consensus algorithm for preserving energy consumption. *Applied Sciences, 11*(15), 6750. https://doi.org/10.3390/app11156750

Kara, M., Laouid, A., Hammoudeh, M., AlShaikh, M., & Bounceur, A. (2022). Proof of Chance: A lightweight consensus algorithm for the Internet of Things. *IEEE Transactions on Industrial Informatics, 18*(11), 8336–8345. https://doi.org/10.1109/TII.2022.3168747

Karantias, K., Kiayias, A., & Zindros, D. (2020). Proof-of-burn. *In International Conference on Financial Cryptography and Data Security* (pp. 523–540). Springer.

King, S., & Nadal, S. (2012). PPcoin: Peer-to-peer crypto-currency with proof-of-stake. Self-Published Paper, 1–6.

Milutinovic, M., He, W., Wu, H., & Kanwal, M. (2016). Proof of luck: An efficient blockchain consensus protocol. *In Proceedings of the 1st Workshop on System Software for Trusted Execution* (pp. 1–6). https://doi.org/10.1145/3007788.3007790

Mudassir, M., Bennbaia, S., Unal, D., & Hammoudeh, M. (2020). Timeseries forecasting of bitcoin prices using high-dimensional features: A machine learning approach. *Neural Computing and Applications, 32*, 13787–13798.

Nijsse, J., & Litchfield, A. (2020). A taxonomy of blockchain consensus methods. *Cryptography, 4*(4), 32. https://doi.org/10.3390/cryptography4040032

Prasad, K. H. V., & Periyasamy, S. (2023). Secure-energy efficient bio-inspired clustering and deep learning-based routing using blockchain for edge assisted WSN environment. *IEEE Access, 11*, 145421–145440. https://doi.org/10.1109/ACCESS.2023.3345218

Rathi, V. K., et al. (2020). A blockchain-enabled multi domain edge computing orchestrator. *IEEE Internet of Things Magazine, 3*(2), 30–36. https://doi.org/10.1109/IOTM.0001.1900089

Salimitari, M., & Chatterjee, M. (2018). A survey on consensus protocols in blockchain for IoT networks. *arXiv Preprint arXiv*:1809.05613. https://arxiv.org/abs/1809.05613

Shoker, A. (2017). Sustainable blockchain through proof of exercise. *In Proceedings of the IEEE 16th International Symposium on Network Computing and Applications* (pp. 1–9). https://doi.org/10.1109/NCA.2017.8171374

Upadhyay, V., Vaish, A., & Kokila, J. (2024). The need for lightweight consensus algorithms in IoT environment: A review. *In Proceedings of the Sixteenth International Conference on Contemporary Computing* (IC3-2024) (pp. 366–376). Association for Computing Machinery. https://doi.org/10.1145/3675888.3676072

Wu, Y., Song, P., & Wang, F. (2020). Hybrid consensus algorithm optimization: A mathematical method based on POS and PBFT and its application in

blockchain. *Mathematical Problems in Engineering, 2020*, 1–13. https://doi.org/10.1155/2020/7270624

Xiaolong, X., et al. (2022). Service offloading with deep Q-network for digital twinning-empowered internet of vehicles in edge computing. *IEEE Transactions on Industrial Informatics, 18*(2), 1414–1423. https://doi.org/10.1109/TII.2021.3095193

Yang, F., Zhou, W., Wu, Q. Q., Long, R., Xiong, N. N., & Zhou, M. (2019). Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism. *IEEE Access, 7*, 118541–118555. https://doi.org/10.1109/ACCESS.2019.2936282

How to cite this Article:

Durgesh Kumar and Shiva Prakash (2026). A Lightweight Proof-of-Chance Blockchain Framework for Secure Healthcare IoT. *International Journal of Experimental Research and Review, 50*, 119-133.

DOI : https://doi.org/10.52756/ijerr.2026.v50.010

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.